UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/469,505	12/22/1999	ROBERT J. STONE	UUN99006	5044

25537 7590 09/30/2003

WORLDCOM, INC.
TECHNOLOGY LAW DEPARTMENT
1133 19TH STREET NW
WASHINGTON, DC 20036

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	14

DATE MAILED: 09/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/469,505	Applicant(s) STONE ET AL.	
	Examiner Christian La Forgia	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *12* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☒ Other: *PTO-1533* .

Rule § 1.105 Requirements for Information

1. Applicant and the assignee of this application are required under 37 CFR 1.105 to provide the following information that the examiner has determined is reasonably necessary to the examination of this application.

2. In response to this requirement, please provide copies of each publication which any of the applicants authored or co-authored and which describe the disclosed subject matter of tracking denial of service floods, such as the presentation given by Robert Stone on 05 October 1999, including any materials, notes, or other documentation used to prepare the presentation.

3. In response to this requirement, please provide the title, citation and copy of each publication that any of the applicants relied upon to draft the claimed subject matter, including the presentation given by Robert Stone on 05 October 1999 as an example. For each publication, please provide a concise explanation of the reliance placed on that publication in distinguishing the claimed subject matter from the prior art.

4. The fee and certification requirements of 37 CFR 1.97 are waived for those documents submitted in reply to this requirement. This waiver extends only to those documents within the scope of this requirement under 37 CFR 1.105 that are included in the applicant's first complete communication responding to this requirement. Any supplemental replies subsequent to the first communication responding to this requirement and any information disclosures beyond the scope of this requirement under 37 CFR 1.105 are subject to the fee and certification requirements of 37 CFR 1.97.

5. The applicant is reminded that the reply to this requirement must be made with candor and good faith under 37 CFR 1.56. Where the applicant does not have or cannot readily obtain

an item of required information, a statement that the item is unknown or cannot be readily obtained will be accepted as a complete reply to the requirement for that item.

6. This requirement is an attachment of the enclosed Office action. A complete reply to the enclosed Office action must include a complete reply to this requirement. The time period for reply to this requirement coincides with the time period for reply to the enclosed Office action.

DETAILED ACTION

7. Claims 1 through 29 are presented for examination.

Drawings

8. The drawings received on 22 December 1999 are accepted by the Examiner.

9. The Patent and Trademark Office no longer makes drawing changes. See 1017 O.G. 4. It is applicant's responsibility to ensure that the drawings are corrected. Corrections must be made in accordance with the instructions below.

INFORMATION ON HOW TO EFFECT DRAWING CHANGES

Replacement Drawing Sheets

Drawing changes must be made by presenting replacement figures which incorporate the desired changes and which comply with 37 CFR 1.84. An explanation of the changes made must be presented either in the drawing amendments, or remarks, section of the amendment. Any replacement drawing sheet must be identified in the top margin as "Replacement Sheet" and include all of the figures appearing on the immediate prior version of the sheet, even though only one figure may be amended. The figure or figure number of the amended drawing(s) must not be labeled as "amended." If the changes to the drawing figure(s) are not accepted by the examiner, applicant will be notified of any required corrective action in the next Office action. No further drawing submission will be required, unless applicant is notified.

Identifying indicia, if provided, should include the title of the invention, inventor's name, and application number, or docket number (if any) if an application number has not been assigned to the application. If this information is provided, it must be placed on the front of each sheet and centered within the top margin.

Annotated Drawing Sheets

A marked-up copy of any amended drawing figure, including annotations indicating the changes made, may be submitted or required by the examiner. The annotated drawing sheets must be clearly labeled as "Annotated Marked-up Drawings" and accompany the replacement sheets.

Timing of Corrections

Applicant is required to submit acceptable corrected drawings within the time period set in the Office action. See 37 CFR 1.85(a). Failure to take corrective action within the set period will result in ABANDONMENT of the application.

If corrected drawings are required in a Notice of Allowability (PTOL-37), the new drawings MUST be filed within the THREE MONTH shortened statutory period set for reply in the "Notice of Allowability." Extensions of time may NOT be obtained under the provisions of 37 CFR 1.136 for filing the corrected drawings after the mailing of a Notice of Allowability.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1 through 8, 10 through 20, 22 through 24, and 26 through 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 6,301,668 to Gleichauf et al., hereinafter Gleichauf, in view of United States Patent No. 6,014,628 to Kovarik, Jr., hereinafter Kovarik.

12. As per claim 1, Gleichauf teaches a method for tracking denial-of-service floods, the method comprising:

rerouting a DoS flood attack datagram to a tracking router, wherein the tracking router forms an overlay tracking network with respect to an egress edge router (Figure 2 [block 20, 28],

3, 4 [block 110]; column 2, lines 58-60; column 3, lines 7-13; column 4, lines 57-67; column 5, lines 1-32; column 6, lines 14-24). One of ordinary skill in the art could appreciate that the network security system discussed in Gleichauf could be replaced by a tracking router in order to provide a similar function as sought by the present claim limitations, namely that of forming a tracking network to discover where the attack is directed. Gleichauf provides for this function by maintaining a network map in order to discover the profile of the attack, namely in this instance a denial-of-service flood attack.

13. Gleichauf does not teach:

identifying an ingress edge router that forwarded the DoS flood attack datagram.

14. Kovarik teaches:

identifying an ingress edge router that forwarded the DoS flood attack datagram (Figure 1 [blocks 12b], 2, 5 [block 100], 7 [block 102], 10 [block 208, 216, 220]; column 2, lines 33-47; column 3, lines 3-14; column 11, lines 64-66column 12, lines 16-39). It would have been obvious to one of ordinary skill in the art at the time the invention was made to identify the ingress router that forwarded the DoS flood attack. One would be motivated to include the identification of the ingress router because it would aid in creating an attack signature, which could be further used to prevent similar attacks from occurring. For further discussion on the matter of attack signatures please refer to Gleichauf, column 6, lines 37 to 45.

15. Regarding claim 2, Gleichauf teaches further comprises executing security diagnostic functions (Figure 1 [block 2], 2 [block 20], 4 [blocks 106, 108]; column 2, lines 43-55).

16. With regards to claims 3 and 15, Gleichauf teaches wherein the security diagnostic functions comprise input debugging (Figure 4 [blocks 106, 108]; column 7, line 66 to column 8, line 45).

17. Regarding claims 4 and 16, Gleichauf teaches wherein the overlay tracking network is within an autonomous system that is different from another autonomous system corresponding to the ingress edge router and the egress edge router (Figure 1 [block 6], 2 [block 28], 4 [block 110]; column 4; lines 24-33; column 7, line 66 to column 8, line 27).

18. With regards to claims 5, 11, and 17, Kovarik teaches further comprising providing routing information by the overlay tracking network to the ingress edge router and the egress edge router using an inter-administrative-domain routing/signaling protocol (Figure 10 [blocks 208, 216, 220]; column 13, lines 21-38). Motivation for combining Kovarik with the system of Gleichauf is discussed above.

19. Concerning claims 6, 12, and 18, Kovarik teaches wherein the inter-administrative-domain routing/signaling protocol is BGP (Border Gateway Protocol) (Figure 10 [blocks 208, 216, 220]; column 13, lines 21-38). Border Gateway Protocol and External Border Gateway Protocol are defined by **Microsoft Computer Dictionary 5th Edition** as a protocol for distributing information regarding availability to the routers and gateways that interconnect networks. Therefore, one of ordinary skill in the art would recognize that using BGP is inherent

to the system of Kovarik as per the discussion in column 13, lines 21 through 38. Motivation for combining Kovarik with the system of Gleichauf is discussed above.

20. Regarding claims 7, 19, and 23, Kovarik teaches further comprising communicating between the edge routers and the tracking router via tunnels that are created over an unreliable datagram delivery service protocol (Figure 2 [block 12b], 10 [blocks 208, 216, 220]; column 6, lines 4-13; column 13, lines 21-38). One of ordinary skill in the art would appreciate that both Kovarik and Gleichauf communicate via computer networking systems, which commonly employ the Internet Protocol (IP), which is commonly recognized as a connectionless oriented protocol. Connectionless oriented protocols are commonly recognized as unreliable delivery protocols, as described on page 97 of **Internetworking with TCP/IP Principles, Protocols, and Architectures 4th Edition**, by Douglas E. Comer.

21. Regarding claims 8, 20, and 24, Gleichauf teaches further comprising communicating between the edge routers and the tracking router via virtual connections over a separate lower layer protocol (column 6, lines 25-36). One of ordinary skill in the art would appreciate that both Kovarik and Gleichauf communicate via computer networking systems, which commonly employ the Internet Protocol (IP), which is a lower level protocol.

22. Regarding claim 10, Kovarik teaches further comprising routing the DoS flood attack datagram from the ingress edge router to the tracking router, wherein the egress edge router has a static route to the victim (Figure 10 [block 210]; column 13, lines 38-44). One of ordinary skill

in the art would recognize that an egress router may have a static route to a victim, if the victim node in question is directly related to one of either a firewall, router or function server on the Internet, such as an FTP or Web server.

23. Concerning claims 13 and 27, Kovarik teaches further comprising establishing another static route between the egress router and an external router associated with a victim node, the victim node receiving the DoS flood attack datagram (Figure 10 [block 210]; column 13, lines 38-44). One of ordinary skill in the art would recognize that an egress router may have a static route to a victim, if the victim node in question is directly related to one of either a firewall, router or function server on the Internet, such as an FTP or Web server.

24. As per claim 14, Gleichauf teaches a communication system for tracking denial-of-service (DoS) floods, the communication system comprising:

a plurality of edge routers including an ingress edge router and an egress edge router, each of the edge routers being configured to perform security diagnostic functions, in part, to identify a DoS flood attack datagram, wherein the ingress edge router is associated with a source of the DoS flood attack datagram (Figure 2 [block 20, 28], 3, 4 [block 110]; column 2, lines 58-60; column 3, lines 7-13; column 4, lines 57-67; column 5, lines 1-32; column 6, lines 14-24). One of ordinary skill in the art could appreciate that the Internet comprises a plurality of edge routers configured to perform security diagnostic functions, in particular to identify DoS attacks. Furthermore, it is commonly known in the art that said routers are programmed to identify the originator of the DoS flood attack.

25. Gleichauf does not teach a tracking router adjacent to the egress edge router, the tracking router being configured to perform the security diagnostic functions, the ingress edge router rerouting the DoS flood attack datagram to the tracking router as to permit identification of the ingress edge router, wherein the tracking router forms an overlay tracking network with respect to the plurality of edge routers.

26. Kovarik teaches a tracking router adjacent to the egress edge router, the tracking router being configured to perform the security diagnostic functions, the ingress edge router rerouting the DoS flood attack datagram to the tracking router as to permit identification of the ingress edge router, wherein the tracking router forms an overlay tracking network with respect to the plurality of edge routers (Figure 1 [blocks 12b], 2, 5 [block 100], 7 [block 102], 10 [block 208, 216, 220]; column 2, lines 33-47; column 3, lines 3-14; column 11, lines 64-66column 12, lines 16-39). With respect to the overlay tracking network, it is understood that Gleichauf teaches that particular limitation as per the abovementioned discussion. It would have been obvious to one of ordinary skill in the art at the time the invention was made to identify the ingress router that forwarded the DoS flood attack. One would be motivated to include the identification of the ingress router because it would aid in creating an attack signature, which could be further used to prevent similar attacks from occurring. For further discussion on the matter of attack signatures please refer to Gleichauf, column 6, lines 37 to 45.

27. Regarding claim 22, Kovarik teaches wherein the overlay tracking network further comprises additional tracking routers (Figure 10 [blocks 208, 216, 220]; column 13, lines 21-38).

28. Regarding claim 26, Gleichauf teaches wherein the ingress edge router routes the DoS flood attack datagram to the tracking router due to a dynamic routing update from the tracking router (Figure 4 [block 110]; column 5, line 52 to column 6, line 23).

29. As per claim 28, Gleichauf teaches a computer-readable medium carrying one or more sequences of one or more instructions for tracking denial-of-service floods (DoS), the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving a DoS flood attack datagram (column 4, lines 40-57; column 6, lines 37-50; column 8, lines 46-58);

identifying the DoS flood attack datagram (column 8, lines 46-58; column 6, lines 37-50).

30. Gleichauf does not teach:

identifying a previous hop router associated with the DoS flood attack datagram to ultimately locate an ingress adjacency and an ingress adjacency associated with the DoS flood attack.

31. Kovarik teaches:

identifying a previous hop router associated with the DoS flood attack datagram to ultimately locate an ingress adjacency and an ingress adjacency associated with the DoS flood attack (Figure 1 [blocks 12b], 2, 5 [block 100], 7 [block 102], 10 [block 208, 216, 220]; column 2, lines 33-47; column 3, lines 3-14; column 11, lines 64-66column 12, lines 16-39). It would have been obvious to one of ordinary skill in the art at the time the invention was made to identify the ingress router that forwarded the DoS flood attack. One would be motivated to

include the identification of the ingress router because it would aid in creating an attack signature, which could be further used to prevent similar attacks from occurring. For further discussion on the matter of attack signatures please refer to Gleichauf, column 6, lines 37 to 45.

32. Regarding claim 29, Kovarik teaches wherein the computer readable medium further includes instructions for causing the one or more processors to perform the steps of:

instructing the previous hop router to identify a respective previous hop router associated with the DoS flood attack datagram (Figure 1 [blocks 12b], 2, 5 [block 100], 7 [block 102], 10 [block 208, 216, 220]; column 2, lines 33-47; column 3, lines 3-14; column 11, lines 64-66column 12, lines 16-39).

33. Claims 9, 21, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf in view of Kovarik as applied to claim 1 above, and further in view of United States Patent No. 6,327,242 to Amicangioli et al., hereinafter Amicangioli.

34. Regarding claims 9, 21 and 25, Gleichauf and Kovarik do not teach further comprising communicating between the edge routers and the tracking router via physical connections.

35. Amicangioli teaches further comprising communicating between the edge routers and the tracking router via physical connections (Figure 1, 2, 3, 4, 5, 6, 7; column 2, lines 52-56; column 4, liens 15-19). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the capabilities of the combined system of Gleichauf and Kovarik on a similar invention with a method of establishing a physical connection. One would be motivated to perform such a function as it adds versatility to the combined system of Gleichauf

and Kovarik as it allows the combined system to be applicable to network backbones, particularly those that operate ATM backbones.

Conclusion

36. This Office action has an attached requirement for information under 37 CFR 1.105. A complete reply to this Office action must include a complete reply to the attached requirement for information. The time period for reply to the attached requirement coincides with the time period for reply to this Office action.

37. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

38. The following patents are cited to further show the state of the art with respect to tracking denial of service attacks, such as:

United States Patent No. 6,535,227 to Fox et al., which is cited to show a method for assessing the security posture of a network.

United States Patent No. 6,182,226 to Reid et al., which is cited to show a method for controlling interactions between networks.

United States Patent No. 6,185,689 to Todd, Sr. et al., which is cited to show a method for network self security assessment.

United States Patent No. 6,157,649 to Peirce et al., which is cited to show a method for coordination and control of data streams that uses virtual tunneling.

United States Patent No. 6,484,203 to Porras et al., which is cited to show hierarchical event monitoring and analysis.

United States Patent No. 6,321,338 to Porras et al., which is cited to show network surveillance.

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

40. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

41. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Christian La Forgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100